UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

DIRK HACKETT, individually and on behalf of all others similarly situated, Plaintiff, v. MNGI DIGESTIVE HEALTH, Defendant.	Case No. 0:24-cv-02971 **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Dirk Hackett ("Plaintiff"), through his attorneys, hereby brings this Class Action individually and on behalf of all others similarly situated (collectively, "Class members"), against Defendant MNGI Digestive Health ("MNGI" or "Defendant"). Plaintiff complains and alleges the following upon personal knowledge as to himself and upon information and belief as to all other matters.

INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data breach that occurred on August 20, 2023, which affected Defendant's inadequately protected computer systems and/or network, and which did result in the unauthorized access to approximately 765,937 individuals' personally identifiable information ("PII") and personal health information ("PHI") (hereinafter the "Data Breach").

2. PII and PHI includes, among other sensitive information, individuals' names, Social Security numbers ("SSNs"), driver's license or state identification numbers, passport numbers, dates of birth, medical information and health insurance information, payment card information, and account numbers.

3. Defendant, MNGI Digestive Health, is a nationally recognized gastroenterology healthcare practice with 11 clinics in the Twin Cities area, spanning both Minnesota and Wisconsin.

4. As a condition of receiving services, Defendant's patients are required to provide and entrust Defendant with sensitive and private information, including PII and PHI. Patients thereafter provide their PII and PHI to Defendant with the reasonable expectation that their sensitive information will be kept confidential and safe from unauthorized disclosure.

5. By taking possession and control of their information, Defendant assumed a duty to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals PII and PHI from unauthorized disclosure.

6. Defendant also has a duty to adequately safeguard its patients' sensitive and private information under industry standards and duties imposed by statutes, including the Health Insurance Portability and Accountability Act ("HIPPA"), Section 5 of the Federal Trade Commission Act ("FTC Act"), and other relevant laws and regulations.

7. Defendant breached its duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

8. On or about August 25, 2023, Defendant detected unauthorized activity within its computer systems and/or network and digital environment. The company began an investigation but did not determine until nearly a year later, on June 7, 2024, that patient information had been accessed.[1] Defendant also retained leading cybersecurity experts and legal counsel to assist in the investigation.[2]

---

[1] https://www.mngi.com/media/721/download?inline= (last visited July 23, 2024).
[2] *Id.*

9. While Defendant claimed to have discovered the breach in August 2023, it did not notify victims of the breach until nearly 11 months later, in July of 2024, when it confirmed that cybercriminals had accessed its systems and the personal information of its patients, and began to mail breach notification letters to victims, including Plaintiff.[3]

10. Presently, Defendant has offered no assurance to Plaintiff and Class members that the sensitive and private information that was accessed in the Data Breach has been recovered or destroyed.

11. The information compromised in the Data Breach was disclosed by Defendant to be patients' names, Social Security numbers ("SSNs"), driver's license or state identification numbers, passport numbers, dates of birth, medical information and health insurance information, payment card information, and account numbers."[4]

12. The exposure of a person's PII and PHI through a data breach substantially increases that person's risk of identity theft, fraud, misappropriation of health insurance benefits, and similar forms of criminal mischief, potentially for the rest of their lives. Mitigation of such risk requires individuals to expend a significant amount of time and money to closely monitor their credit, financial accounts, health records, and email accounts. Mitigation of the risk of misuse of their sensitive and private information may not even be possible.

13. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII and/or PHI was accessed and disclosed. Plaintiff and Class members are now at a substantially increased risk of experiencing misuse of their PII/PHI in the coming years. This action seeks to remedy these failings and their consequences.

14. Plaintiff, on behalf of himself and all other Class members whose PII/PHI was exposed in the Data Breach, assert claims for negligence, negligence *per se*, breach

[3] *Id.*
[4] *Id.*

of fiduciary duty, breach of implied contract, unjust enrichment, invasion of privacy, and breach of Minnesota consumer protection laws and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

15. Plaintiff Dirk Hackett is a natural person who resides in Minneapolis, Minnesota.

16. Plaintiff was at all relevant times a patient at MNGI Digestive Health.

17. Plaintiff received medical treatment from Defendant and was required to submit his personal information to Defendant as a condition of those services and treatment, including his name, address, date of birth, contact information, driver's license information, Social Security number, and full health and financial information.

18. Defendant, MNGI Digestive Health, is a nationally recognized gastroenterology healthcare practice with 11 clinics in the Twin Cities, spanning both Minnesota and Wisconsin and maintains its principal place of business at 3001 Broadway Street NE, Suite #120, Minneapolis, MN 55413.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million dollars, exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

20. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District, regularly conducts business in this

District, and the acts and omissions giving rise to Plaintiff's claims emanated from within this District.

21. Venue is proper under 18 U.S.C. § 1391(b) because Defendant maintains its principal place of business in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant Stores Patient PII/PHI

22. Defendant is a nationally recognized gastroenterology healthcare practice with 11 clinics in the Twin Cities area, spanning both Minnesota and Wisconsin. Defendant specializes in the diagnosis and treatment of adults and children with GI disorders and its board-certified gastroenterologists have expertise in virtually all types of digestive conditions, such as acid reflux disease, heartburn and swallowing disorders, Crohn's disease and ulcerative colitis, hepatitis and liver disease, biologics and infusion therapy, celiac disease, hemorrhoid banding and more.[5]

23. As a condition of treating its patients, Defendant requires that its patients entrust it with sensitive and private information such as patient names, dates of birth, addresses, Social Security number, medical history, and financial information in the ordinary course of its business. Defendant also collects sensitive personal and health information such as PII/PHI.

24. Upon information and belief, Defendant's may also receive private and personal information from individuals within its patients' "circle of care," such as family members, close friends, referring physicians and/or other doctors.

25. Defendant's applicable privacy policy demonstrates that it is aware of its legal obligations to keep PII and PHI confidential and secure, and indeed promises to do just that. Defendant's privacy policy admits that it is "Make certain that medical

[5] https://www.mngi.com/.

information that identifies you is kept private and confidential."[6] Further, Defendant promises it "will not use or disclose your protected health information without your specific written authorization."[7]

26. Despite Defendant's representations about the privacy of its patients' information, it did not employ reasonable security measures to protect its patients' PII and PHI from unauthorized disclosure as demonstrated throughout this Complaint.

27. Upon information and belief, the type of information that Defendant maintains includes, *inter alia*: patients' full name, address, date of birth, Social Security number ("SSN"), credit/debit card information, medical history, insurance information, billing information, medical records, photo identification, and any other information necessary to provide care.

28. Due to the highly sensitive nature of the information Defendant collects and maintains, Defendant is obligated provide confidentiality and adequate security for patient safety through its applicable privacy policy, and otherwise in compliance with statutory privacy requirements.

29. In the course of their relationship, Plaintiff and Class members provided Defendants with at least their PII and/or PHI.

30. Plaintiff and Class members, as current patients of Defendant, relied on Defendant to keep their sensitive PII/PHI confidential and secured, to use such information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

[6] https://www.mngi.com/media/555/download?inline (last accessed July 23, 2024).
[7] *Id.*

31. On or about August 25, 2023, Defendant detected unauthorized activity within its systems. In response, it took steps to secure its network and began an investigation. MNGI also engaged independent cybersecurity experts to assist with the investigative efforts. This investigation determined that unauthorized access to certain portions of its network occurred on August 20, 2023.[8]

32. Not until June 7, 2024, however, did the Defendant determine that patient information had been accessed by the hackers.[9] Over a month later, on July 15, 2024, Defendant began notifying affected individuals about the Data Breach.

33. In September 2023, the criminal ransomware group, Alphv/BlackCat took responsibility for the attack.[10]

34. Defendant has not acknowledged specifically that Alphv/BlackCat was responsible for the attack.

35. Alphv/BlackCat is a particularly prolific criminal ransomware group that frequently targets the healthcare sector.[11]

36. On or about June 7, 2024, Defendant finally confirmed that the information compromised in the Data Breach included patients' names, Social Security numbers ("SSNs"), driver's license or state identification numbers, passport numbers, dates of

[8] *Supra* n.1.
[9] *Id.*
[10] https://www.securityweek.com/mngi-digestive-health-data-breach-impacts-765000-individuals/ (last visited July 23, 2024).
[11] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a (last visited July 23, 2024).

birth, medical information and health insurance information, payment card information, and account numbers.[12]

37. Defendant began to notify the victims of the breach on July 15, 2024, almost 12 months after the attack occurred.[13]

38. Defendant's failure to promptly notify Plaintiff and Class members that their PII and PHI was compromised placed them at a higher risk that their information will be used towards illegal means since their information was vulnerable for almost 12 months without their knowledge. Due to the delay, Plaintiff and Class members were unable to take affirmative steps to mitigate their risks of fraud and/or identity theft from the unauthorized disclosure of their PII and PHI.

39. Additionally, the breach notification letter is deficient, which quite simply informs victims that their PII and or PHI has been compromised.

> On August 25, 2023, MNGI discovered unauthorized activity within its digital environment. In response, MNGI took steps to secure its network and began an investigation. MNGI also engaged independent cybersecurity experts to assist with the investigative efforts. This investigation determined that unauthorized access to certain portions of our network occurred on August 20, 2023.
>
> MNGI then undertook a comprehensive review of the potentially affected data. On June 7, 2024, MNGI identified that certain individuals' personal and/or protected health information was potentially affected. The potentially affected information may include individuals' names, Social Security numbers, driver's license or state identification numbers, passport numbers, dates of birth, medical information and health insurance information, payment card information, and account numbers. On July 15, 2024, MNGI provided written notification of the incident via US mail to impacted individuals.

[12] *Supra* n.1.
[13] *Id.*

> MNGI has implemented additional measures to enhance network security and minimize the risk of a similar incident occurring in the future.
>
> MNGI has established a toll-free call center to answer questions about the incident and to address related concerns. Call center representatives are available Monday through Friday between 9am – 9pm EST and can be reached at 888-326-0965.
>
> While we are not aware of the misuse of any potentially affected individual's information, we are providing the following information to help those wanting to know more about steps they can take to protect themselves and their personal information:[14]

40. Notably, the breach notification letter fails to adequately describe with specificity the nature of the attack and the measures taken by Defendant, if any, to prevent future attacks. Without these details, Plaintiff and Class members are at a disadvantage to take steps to mitigate the harms resulting from the Data Breach.

41. Instead, Defendant vaguely states that it has taken steps to make sure a similar incident does not happen again without any additional details.

42. The mitigation efforts offered by Defendant in the breach notification letter are also wholly deficient.

43. Defendant offers only pro forma advice on how to freeze your credit and put a fraud alert on your accounts, which is inadequate to redress the damage to Plaintiff and Class members' privacy and the imminent threat they now face and will likely continue to face for the remainder of their lives.

44. Defendant wishes to place the burden of identity protection on Plaintiff and Class members when the blame for the access and disclosure of their PII and PHI is through no fault of their own. Rather, it is Defendant's fault.

---

[14] *Id.*

45. Based on the unfortunate events described throughout this Complaint, Defendant failed to take action to prevent the Data Breach by implementing data security measures to protect its network from unauthorized breach and thereby failed to protect its patients' PII and PHI.

46. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a healthcare entity that collects, creates, and maintains PII/PHI on its computer network and/or systems.

47. Plaintiff's and Class members' PII and PHI was compromised and acquired in the Data Breach.

48. Plaintiff further believes that his PII and PHI will continue to be available for purchase on the dark web, which is the *modus operandi* of cybercriminals.

49. Plaintiff and Class members now face a heightened and continued threat of identity theft and other types of criminal mischief resulting from the Data Breach.

Defendant Knew that PII/PHI is Valuable to Cybercriminals and Failed to Take Action to Prevent its Theft

50. At all relevant times, Defendant knew, or should have known, that Plaintiff's and Class members' PII/PHI was a target for cybercriminals. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyberattacks.

51. By acquiring, collecting, and using Plaintiff's and Class members PII/PHI, Defendant assumed legal and equitable duties created by the HIPPA, the FTC Act,

industry standards, contract, and statutory and common law to keep Plaintiff's and Class members PII/PHI confidential, and to protect it from unauthorized access and disclosure.

52. Additionally, Defendant's data security obligations were of particular importance due to the steady increase over the years of data breaches targeting medical information.

53. The healthcare industry is a known target for cyber criminals. "High demand for patient information and often-outdated systems are among the nine reasons healthcare is not the biggest target for online attacks."[15] They are also more likely to pay for a hacker's ransom due to the sensitive information that they maintain and collect, and an incentive to regain access to their data quickly.[16]

54. The number of data breaches experienced by healthcare entities continues to rise. In a 2024 report, the healthcare compliance company Protenus found that there were 942 medical data breaches in 2023, leaving over 171 million patient records exposed. This is an increase from the 905 medical data breaches that Protenus compiled in 2021.[17]

---

[15] Swivel Secure, *The healthcare industry is at risk*, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited July 23, 2024).

[16] Elise Takahama, *Why health care has become a top target for cybercriminals*, The Seattle Times (Feb. 25, 2024), https://www.seattletimes.com/seattle-news/health/why-health-care-has-become-a-top-target-for-cybercriminals/. (last visited July 17, 2024).

[17] *2024 Breach Barometer*, PROTENUS, available for download at: https://www.protenus.com/breach-barometer-report (last visited July 23, 2024).

55. According to Mimecast, a cybersecurity firm, 90% of healthcare organizations experienced cyberattacks in 2020.[18]

56. In fact, the last several years are marked by several high-profile healthcare data breaches including:

- Eastern Radiologists, Inc. (886,746 patients, February 2024);
- MCNA Dental (8,900,000 patients, March 2023);
- Broward Health (1,300,000 patients, January 2022);
- Morley (521,046 patients, February 2022);
- Regal Medical Group (3,300,000 patients, December 2022);
- Trinity Health (3,300,000 patients, March 2020);
- Shields Healthcare Group (2,000,000 patients, March 2022); and
- One Touch Point (2,600,000 individuals, July 2022).

57. An article from April 23, 2024 discussed the latest findings in Baker Hostetler's tenth annual Data Security Incident Response Report, which found that despite companies' adeptness to respond to cyberattacks from criminals, "ransomware attacks show no signs of abating…"[19] Moreover, "Combating these attacks has also been complicated by hackers' practice of constantly innovating and evolving their methods in

[18] Maria Hernandez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988- iowa-city-hospital-suffers-phishing-attack (last visited July 23, 2024).

[19] Allison Grande, *Ransomware Still on the Rise Despite Better Defenses, Firm Says*, LAW 360 (Apr. 23, 2024), https://www.law360.com/articles/1827647/ransomware-still-on-rise-despite-better-defenses-firm-says (last visited July 23, 2024).

order to get around the controls and safeguards that businesses are erecting to counter their attacks…"[20]

58. Additionally, the U.S. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Multi-State Information Sharing and Analysis Center issued an alert about Alphv/BlackCat, the cybercriminals responsible for this Data Breach, which was revised in February 2024.[21] The warning disseminated key information about the ransomware group including indicators of compromise, detection methods, tactics, techniques, and procedures used.[22] The warning also alerted the public that Alphv/BlackCat has in the past particularly targeted organizations in the healthcare sector.[23]

59. Defendant certainly knew and understood that unprotected or exposed PII/PHI in the custody of healthcare entities, like Defendant, is valuable and highly sought after by criminals seeking to illegally monetize that PII/PHI through unauthorized access.

60. Indeed, personal data such as PII/PHI is a valuable property right, leading to the purchase of said data by American companies. American companies have spent over $19 billion on acquiring personal data of consumers in 2018.[24]

---

[20] *Id.*
[21] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a (last visited July 23, 2024).
[22] *Id.*
[23] *Id.*
[24] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited July 23, 2024).

61. Consumers also place a high value on the privacy of their data. Studies confirmed that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[25] Recently, more consumers are exercising their Data Subject Access Rights and leaving providers over their data practices and policies.[26]

62. Considering the value behind PII/PHI, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

63. PII/PHI is also of high value to identity thieves, as evidenced by their practice of trading such private information including, SSNs, on the black market or "dark web." PII/PHI is a measurable commodity on the black market.[27] PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[28] In 2021, it was

[25] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available for download at: https://www.jstor.org/stable/23015560?seq=1.

[26] CISCO, *Cisco 2023 Consumer Privacy Survey* (April 2023), available at https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html?CCID=cc000742.

[27] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited July 23, 2024).

[28] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited July 23, 2024).

reported that stolen healthcare records can also fetch for as much as $1000 on the black market.[29] That price is likely much higher today.

64. According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[30]

65. Another report demonstrates that cybercriminals continue to profit from ransomware attacks: "The largest ransom paid in 2023 was more than $10 million, an increase from the $8 million payment high from 2022, and the average ransom paid in 2023 was $747,651, which nearly matches the average payment high that was set in 2020 during the height of the ransomware epidemic, the report noted."[31]

66. Companies like Defendant are aware that consumers value the privacy of their sensitive data such as PII/PHI and that cybercriminals continue to successfully target that data to obtain significant profits. As such, companies like Defendant remain on high alert and must act in accordance with their legal and equitable obligations to implement reasonable security measures to prevent targeted data attacks aimed at their patients' PII/PHI.

---

[29] Paul Nadrag, *Industry Voices-Forget credit card numbers. Medical records are the hottest items on the dark web*, FIERCE HEALTHCARE (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web) (last visited July 23, 2024).

[30] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[31] *Supra* n.19.

67. Armed with this knowledge, Defendant breached its duties by failing to implement and maintain reasonable security measures to protect Plaintiff's and Class members' PII/PHI from being stolen.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

68. The theft of PII/PHI is costly for those affected. A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[32] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[33]

69. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, identity theft can happen in many ways: fraudsters can obtain and sell personal data to other criminals, or use personal data to open a new credit card or loan, open a bank account and write bad checks, apply for government benefits, take over existing debit and credit accounts, withdraw funds, and even get medical procedures.[34]

---

[32] *Supra* n.28.

[33] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited July 23, 2024).

[34] Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited July 23, 2024).

70. The Federal Trade Commission ("FTC") also warns consumers about the type of fraud that identity thieves use PII/PHI to achieve.[35] Criminals can also obtain a driver's license or official identification card in the victim's name, but with the thief's picture, use the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[36]

71. Alarmingly, a thief can use stolen medical information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[37]

72. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a week to resolve issues stemming from identity theft and some need months to a year.[38]

73. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[35] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited July 23, 2024).

[36] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited July 23, 2024).

[37] *Supra* n.28.

[38] Identity Theft Resource Center, 2023 Consumer Impact Report, available for download at: https://www.idtheftcenter.org/publications/.

74. Victims of medical identity theft face another set of problems. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected;
- Significant bills for medical goods and services not sought nor received;
- Issues with insurance, co-pays, and insurance caps;
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft;
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime;
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts;
- Phantom medical debt collection based on medical billing or other identity information; and
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[39]

75. Further complicating victims' ability to defend themselves from identity theft is the time lag between when PII/PHI is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers

[39] World Privacy Forum, *The Geography of Medical Identity Theft* (Dec. 12, 2017), available for download at: https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/.

to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[40]

76. Plaintiff and Class members now live with their PII/PHI exposed in cyberspace and available to people willing to purchase and use the information for any number of improper purposes and crimes.

77. Plaintiff and Class members now face constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages, in addition to any fraudulent use of their PII/PHI.

Defendant Failed to Comply with Statutory Regulations

78. The Health Insurance Portability and Accountability Act ("HIPPA") requires covered entities to implement reasonable security measures to protect patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

79. HIPPA further prohibits the unauthorized disclosure of protected health information.

[40] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), available at: http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf

80. Defendant is a HIPPA covered entity that provides healthcare services. *See* 45 C.F.R. § 160.12. As a regular and necessary part of its business, Defendant collects and maintains the PII/PHI of patients.

81. HIPPA requires Defendant to implement adequate safeguards to prevent unauthorized use or disclosure of private information such as PII/PHI by adopting the requirements set forth in the HIPPA's Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information), and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

82. Defendant is also required to report any unauthorized use or disclosure of that information, including incidents of a data breach "without unreasonable delay and in no case later than 60 days following discovery of the breach."[41] *See* 45 C.F.R. § 164.302.

83. As a HIPPA covered entity, Defendant assumed legal obligations and knew or should have known that it was responsible for safeguarding Plaintiff's and Class members' sensitive and private information from unauthorized disclosure.

84. As set forth throughout this Complaint, Defendant did not implement the required safeguards it is required to maintain under HIPPA. Defendant did so with knowledge of its legal duties under HIPPA and of the risks associated with unauthorized access to Plaintiff's and Class members' PHI.

[41] Breach Notification Rule, U.S. Dep't of Health & Human Services, available at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

85. Defendant's HIPPA violations include but are not limited to the following:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits. 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of PHI. 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosure of electronic PHI that is not permitted. 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPPA security standards by Defendant's workforce. 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations. 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate the harmful effects of security incidents that are known. 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry our their functions and to maintain security of PHI. 45 C.F.R. § 164.530(b); 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI. 45 C.F.R. § 164.530(c).

86. As a result of their failure to comply with HIPPA regulations, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach and injuring Plaintiff and Class members.

87. The Federal Trade Commission Act ("FTC Act") prohibits Defendant from engaging in "unfair or deceptive acts or practices in or affecting commerce." *See* 15 U.S.C. § 45.

88. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which reflect the importance of implementing reasonable data security practices.

89. The FTC's publication, *Protecting Personal Information*, established cyber-security guidelines for businesses. The guidelines provide that businesses should take action to protect the personal patient information that they collect; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems.[42]

90. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[43]

91. The FTC further recommends that businesses not maintain private information longer than is needed for authorization of a transaction; limit access to

[42] *Protecting Personal Information: A Guide for Business, Federal Trade Commission* (2016). Available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[43] *Id.*

sensitive information; require complex passwords be used on networks; use industry-tested methods for security monitor for suspicious activity on the networks; and verify that third-party service providers have implemented reasonable security measures.

92. The FTC has the authority to bring enforcement actions against businesses for failing to protect PII/PHI adequately and reasonably under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

93. The orders that result from enforcement actions further clarify the measures businesses must take to meet their data security obligations.

94. Defendant failed to properly implement basic data security practices.

95. Defendant was at all relevant times fully aware of its obligations to protect patients' PII/PHI, and of the significant consequences that would result from its failure to do so.

96. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

97. Consequently, cybercriminals circumvented Defendant's lax security measures, resulting in the Data Breach.

Defendant Failed to Comply with Industry Standards

98. Industry standards for healthcare providers such as Defendant exist because of the high threat of cyberattacks that target the sensitive information that they collect and maintain.

99. These practices include but are not limited to: educating and training employees about the risks of cyberattacks, strong passwords, multi-layer security such as firewalls, anti-virus and malware software, encryption, multi-factor authentication, backup data, limitation of employees with access to sensitive data, setting up network firewalls, switches and routers, monitoring and limiting the network ports, and monitoring and limited access to physical security systems.

100. Defendant failed to meet the minimum standards of any of the following: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

101. Defendant's failure to implement the industry standards described herein resulted in the Data Breach and caused injury to Plaintiff and Class members.

Common Damages Sustained by Plaintiff and Class Members

102. For the reasons mentioned above, Plaintiff and Class members have suffered injury and damages directly attributable to Defendant's failure to implement and maintain adequate security measures, including, but not limited to: (i) fraudulent bank accounts opened in their name (ii) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) invasion of their privacy; (v) deprivation of the value

of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

Plaintiff Dirk Hackett's Experience

103. Plaintiff Dirk Hackett is a patient of Defendant.

104. As a condition of receiving medical treatment from Defendant, Plaintiff was required to provide private information to Defendant including his name, address, email address, driver's license information, Social Security number, and full health and financial information.

105. Upon information and belief, Defendant retained Plaintiff's private information in its system at the time of the Data Breach.

106. On June 7, 2024, Plaintiff received a notice letter from Defendant which identified his as a victim whose "personal and protected health information was potentially affected by this incident."

107. The letter disclosed that information stolen was stated to be Plaintiff's "name and Medical Information."

108. Plaintiff is careful about sharing his private information. Plaintiff stores any documents containing private information in a safe and secure location. Plaintiff would not have entrusted his private information with Defendant had he known of Defendant's failure to implement and maintain data security measures.

109. Plaintiff's PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the Data Breach.

110. Since the announcement of the Data Breach, Plaintiff have been required to spend valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII/PHI, time they would not have had to spend but for the Data Breach.

111. Indeed, around the time of the Data Breach, Plaintiff received notification from his bank that unauthorized purchases were attempted on his banking card, thereby heightening the need for him to spend time to carefully monitor the fraud.

112. As a result of the Data Breach, Plaintiff suffered actual injury including, but not limited to: (i) fraudulent bank accounts opened in their name; and (ii) a substantially increased risk of identity theft and medical theft; (iii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) invasion of their privacy; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

113. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which is amplified by the fact that key details about the Data Breach are still unknown, and Plaintiff's PII/PHI is still at risk of being stolen and used for fraudulent activity.

CLASS ALLEGATIONS

114. Plaintiff brings this class action individually and on behalf of all persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

115. Plaintiff seeks certification of a Class as defined below and subject to further amendment:

> **Nationwide Class**
>
> All individuals in the United States whose PII and/or PHI was compromised in the Data Breach that occurred on August 20, 2023 (the "Class").
>
> **State Subclass**
>
> All individuals residing in Minnesota whose PII and/or PHI was compromised in the Data Breach that occurred on August 20, 2023 (the "Minnesota Subclass").

116. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

117. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

118. Numerosity. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. It has been reported to the Maine Attorney General that approximately 765,937 people were affected by the Data Breach. The contact information of those individuals is available from Defendant's business records.

119. Commonality. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

c. Whether Defendant breached its duties to protect Plaintiff's and Class members' PII/PHI;

d. Whether Defendant breached its fiduciary duty to Plaintiff and Class members;

e. When Defendant learned of the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring procedures were deficient;

g. Whether hackers obtained Plaintiff's and Class members' data in the Data Breach;

h. Whether an implied contract existed between Plaintiff, Class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

i. Whether Defendant was unjustly enriched;

j. Whether Defendant's conduct violates the Minnesota Consumer Fraud Act, Minn. Stat. §§ 325F.68, et seq. and Minn. Stat. §§ 8.31, et seq.;

k. Whether Defendant's conduct violates the Minnesota Health Records Act, Minn. Stat. § 144.291, et seq.;

l. Whether Plaintiff and Class members are entitled to injunctive relief and identity theft protection to redress the imminent harm they face due to the Data Breach; and

m. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

120. Typicality. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

121. Adequacy of Representation. Plaintiff will fairly and adequately protect the interests of Class members. Plaintiff is an adequate representative of the Class in that they have no interests adverse to, or conflict with, the Class they seek to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

122. Superiority. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to

be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

123. All members of the proposed Class are readily ascertainable. Defendant has access to the names, addresses, and/or email addresses of Class members affected by the Data Breach.

124. Finally, class certification is appropriate under Fed. R. Civ. P. 23(b). Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(Plaintiff, on behalf of himself and the Nationwide Class, or in the alternative, the Minnesota Subclass)

125. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

126. Defendant requires that its patients, including Plaintiff and Class members, submit private information such as PII and PHI in the course of providing its medical services.

127. Defendant collected, acquired, and stored Plaintiff's and Class members' private information.

128. Plaintiff and Class members entrusted Defendant with their private information and had the understanding that Defendant would safeguard their information.

129. Defendant had knowledge of the sensitivity of Plaintiff's and Class members' private information, and the consequences that would result from the unauthorized disclosure of such information. Defendant knew that healthcare entities were the target of cyberattacks in the past, and that Plaintiff and Class members were the foreseeable and probable victims of any inadequate data security procedures.

130. It was therefore reasonably foreseeable that the failure to implement adequate data security procedures would result in injuries to Plaintiff and Class members.

131. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their private information in its possession, custody, or control from the unauthorized disclosure of such information.

132. Defendant's duty to exercise reasonable care arises from several sources, including but not limited to common law, the HIPPA, the FTC Act, industry standards, and other statutory law.

133. Defendant's duty also arose from its position as a healthcare provider. As a healthcare provider, Defendant assumed a duty to exercise reasonable care in safeguarding and protecting patients' private information in its possession, custody, or control from the unauthorized disclosure of such information.

134. Defendant breached its duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

135. Defendant admitted that the PII/PHI of Plaintiff and Class members was disclosed to unauthorized third persons as a result of the Data Breach.

136. Defendant's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members caused their PII/PHI to be compromised in the Data Breach.

137. Plaintiff and Class members were in no position to protect their PII/PHI themselves.

138. But for Defendant's breach of the duties described herein, Plaintiff and Class members' PII and PHI would not have been compromised.

139. There is a causal relationship between Defendant's failure to implement, control, direct, oversee, manage, monitor, and audit adequate data security procedures to protect the PII and PHI of its patients and the harm suffered by Plaintiff and Class members.

140. Defendant's conduct caused the Data Breach, and as a direct and proximate result, Plaintiff and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) substantially increased risks of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

141. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

142. Plaintiff and Class members are entitled to damages incurred as a result of the Data Breach.

143. Defendant's negligent conduct is ongoing, in that it still holds Plaintiff's and Class members PII and/or PHI in an unsafe and nonsecure manner.

144. Plaintiff and Class Members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class Members.

COUNT II
NEGLIGENCE PER SE
(Plaintiff, on behalf of himself and the Nationwide Class, or in the alternative, the Minnesota Subclass)

145. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

146. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

147. Defendant's duties also arise from Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant of failing to employ reasonable measures to protect and secure PII/PHI.

148. Defendant violated HIPAA Privacy and Security Rules, Section 5 of the FTC Act, UCL, CMIA, and CCPA by failing to use reasonable measures to protect Plaintiff's and Class members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data

breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

149. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTC Act constitute negligence *per se*.

150. Plaintiff and Class members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTC Act were intended to protect.

151. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTC Act were intended to guard against.

152. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

153. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules, and Section 5 of the FTC Act. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to

compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

154. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

155. Plaintiff and Class members are entitled to damages incurred as a result of the Data Breach.

156. Plaintiff and Class members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class members.

COUNT III
BREACH OF FIDUCIARY DUTY
(Plaintiff, on behalf of himself and the Nationwide Class, or in the alternative, the Minnesota Subclass)

157. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

158. Plaintiff and Class members gave Defendant their PII/PHI in confidence, believing that Defendant would protect that information. Plaintiff and Class members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and

Class members' PII/PHI created a fiduciary relationship between Defendant and Plaintiff and Class members. In light of this relationship, Defendant must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

159. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA and the FTC Act, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

160. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) substantially increased risks of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

161. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of

injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

162. Plaintiff and Class Members are entitled to damages incurred as a result of the Data Breach.

163. Plaintiff and Class Members are also entitled to injunctive relief in the form of requiring Defendant to strengthen its data security procedures and to provide credit monitoring to Class Members.

COUNT IV
BREACH OF CONTRACT
(Plaintiff, on behalf of himself and the Nationwide Class, or in the alternative, the Minnesota Subclass)

164. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

165. Plaintiff and Class members entered into contracts with Defendant when they obtained medical services, or otherwise provided PII/PHI to Defendant.

166. In exchange for providing medical services, Defendant promised to safeguard and protect the PII/PHI of Plaintiff and the Class members.

167. Defendant made express promises to Plaintiff and Class members that:

a. Defendant is required by law to "[m]ake certain that medical information that identifies you is kept private and confidential";

b. Defendant will not "will not use or disclose your protected health information without your specific written authorization."; and

c. Defendant "[a]bide by our current Notice of Privacy Practices."

168. These express promises are contained within Defendant's website and/or other materials provided to Plaintiff and Class members upon receiving medical services from Defendant.

169. These promises to Plaintiff and Class members formed the basis of the bargain between Plaintiff and the Class members, on the one hand, and Defendant, on the other.

170. Plaintiff and Class members would not have provided their PII/PHI to Defendant had they known Defendant would not safeguard their PII/PHI.

171. Plaintiff and Class members fully performed their obligations under their contracts with Defendant.

172. Defendant, however, breached its contracts with Plaintiff and the Class members by failing to safeguard Plaintiff's and Class members' PII/PHI.

173. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) substantially increased risks of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) actual identity theft; (iii) improper disclosure of their PII/PHI; (iv) breach of the confidentiality of their PII/PHI; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

174. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

175. Plaintiff and Class members are entitled to damages incurred as a result of the Data Breach.

COUNT V
BREACH OF IMPLIED CONTRACT
(Plaintiff, on behalf of himself and the Nationwide Class, or in the alternative, the Minnesota Subclass)

176. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

177. In connection with obtaining medical services from Defendant, Plaintiff and all other Class members entered into implied contracts with Defendant or were intended third-party beneficiaries of contracts between Defendant and others.

178. Pursuant to these implied contracts, money was paid to Defendant, whether directly from Plaintiff and Class members or their insurance carriers, and Defendant was provided with PII/PHI of Plaintiff and Class members. In exchange, Defendant impliedly agreed to, among other things, take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and protect Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

179. The protection of PII/PHI was a material term of the implied contracts that were either between Plaintiff and Class members, on the one hand, and Defendant,

on the other hand or were between third parties and Defendant to which Plaintiff and Class members were intended third party beneficiaries.

180. Plaintiff and Class members or the third parties fulfilled their obligations under the contracts.

181. Defendant breached its obligations by failing to implement and maintain reasonable data security measures to protect and secure the PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

182. Defendant's breach of its obligations of its implied contracts directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

183. Plaintiff and all other Class members were damaged by Defendant's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face substantially increased risks of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) they suffered actual identity theft; (iv) their PII/PHI was improperly disclosed to unauthorized individuals; (v) the confidentiality of their PII/PHI has been breached; (vi) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vii) they lost time and money to mitigate and remediate the

effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

184. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury, including but not limited to, anxiety, emotional distress, invasion of privacy, and other economic and non-economic losses.

185. Plaintiff and Class members are entitled to damages incurred as a result of the Data Breach.

COUNT VI
UNJUST ENRICHMENT
(Plaintiff, on behalf of himself and the Nationwide Class, or in the alternative, the Minnesota Subclass)

186. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

187. This count is pleaded in the alternative to Plaintiff's breach of contract claims (Counts IV and V).

188. Plaintiff and Class members conferred a monetary benefit upon Defendant in the form of money paid to Defendant and/or its agents for medical services or other services.

189. In exchange, Plaintiff and Class members should have received from Defendant the services that were the subject of the transaction and should have had their private information protected with adequate data security procedures.

190. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members by acquiring and/or collecting their private information as

well as money paid on their behalf as a necessary part of obtaining Defendant's services. Defendant appreciated and benefitted from the receipt of Plaintiff's and Class members' private information and payments in that they used the private information and profited from the healthcare transactions in furtherance of its business.

191. Defendant acquired Plaintiff's and Class members' private information and payments through inequitable means in that it failed to disclose the inadequate data security procedures previously alleged herein.

192. As a result of Defendant's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

193. Defendant should not be permitted to retain the PII/PHI belonging to Plaintiff and Class members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

194. Defendant unjustly enriched itself by using the money and private information acquired from Plaintiff and Class members to further its business.

195. Notably, Defendant chose not to use any payments to enhance their data security procedures.

196. Under principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiff and Class members, and

should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VII
INVASION OF PRIVACY
(Plaintiff, on behalf of himself and the Nationwide Class, or in the alternative, the Minnesota Subclass)

197. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

198. Defendant invaded Plaintiff's and Class members' right to privacy by allowing the unauthorized access to Plaintiff's and Class members' PII/PHI and by negligently maintaining the confidentiality of Plaintiff's and Class members' PII/PHI, as set forth in this Complaint. Defendant further invaded Plaintiff's and Class members' privacy by permitting third parties to access, disclose and publish Plaintiff's and Class members' PII/PHI online.

199. The intrusion was offensive and objectionable to Plaintiff, Class members, and to the reasonable person in that Plaintiff's and Class members' PII/PHI was disclosed without prior written authorization of Plaintiff and other Class members.

200. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class members provided and disclosed their PII/PHI to Defendant privately with an intention that their PII/PHI would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

201. As a direct and proximate result of Defendant's acts described throughout this Complaint, Plaintiff's and the Class members' PII/PHI was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class members suffered damages as described herein.

202. Defendant has committed oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class members' PII/PHI with a willful and conscious disregard of Plaintiff's and the Class members' right to privacy.

203. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and Class members' PII/PHI with sub-standard and insufficient protections without intervention by this Court.

204. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class members great and irreparable injury in that the PII/PHI maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons.

COUNT VIII
VIOLATION OF MINNESOTA CONSUMER FRAUD ACT
Minn. Stat. §§ 325F.68, et seq. and Minn. Stat. §§ 8.31, et seq.
(Plaintiff, on behalf of himself and the Nationwide Class or, in the alternative, the Minnesota Class)

205. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

206. Defendant, Plaintiff, and Class members are each a "person" as defined by Minn. Stat. § 325F.68(3).

207. Defendant's goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

208. Defendant engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

209. Defendant engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of services, in violation of Minn. Stat. § 325F.69(1), including omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII and PHI.

210. The Minnesota Consumer Fraud Act ("MCFA") prohibits "[t]he act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoinable as provided in section 325F.70." Minn. Stat. § 325F.69, subd. 1.

211. Minn. Stat. §8.31, subds. 1 and 3a allows any person injured by a violation of Minn. Stat. § 325F.69 to bring a civil action to recover damages, together with costs and disbursements, including reasonable attorney's fees, and to receive other equitable relief as determined by the court.

212. Defendant engaged in deceptive practices by failing to disclose to Plaintiff and Class members that its data security measures were inadequate to protect their sensitive information.

213. Defendant represented, directly or indirectly, that it maintained appropriate safeguards to protect the personal and medical information of its patients. These representations were false, misleading, and deceptive.

214. Defendant failed to inform Plaintiff and Class members about its deficient data security practices, which constitutes a material omission.

215. Defendant intended that Plaintiff and the Class would rely on its representations and omissions regarding the secure of their personal and medical information.

216. Plaintiff and the Class reasonably relied on Defendant's representations and omissions, believing that their sensitive information was secure.

217. Defendant's deceptive acts and omissions directly caused the exposure of Plaintiff's and Class members' sensitive information in the Data Breach. As a direct and proximate result of the Defendant's deceptive practices, Plaintiff and the Class suffered injuries, including the risk of identity theft, economic losses, loss of privacy, and the need for ongoing credit monitoring and identity theft services.

218. Plaintiff and Class memebrs incurred actual damages due to the exposure of their sensitive information, including but not limited to costs associated with credit monitoring and identity theft protection, economic losses from unauthorized use of their information, and emotional distress. Plaintiff and Class members are entitled to recover statutory damages under Minn. Stat. § 8.31, subd. 3a, due to Defendant's violation of Minn. Stat. § 325F.69.

219. Plaintiff and Class members seek injunctive relief requiring Defendant to implement and maintain reasonable security measures to protect the sensitive information of its patients, to undergo periodic security audits, and to provide appropriate credit monitoring and identity theft protection services to affected individuals.

COUNT IX
VIOLATION OF THE MINNESOTA HEALTH RECORDS ACT
Minn. Stat. § 144.291 *et seq*.
(Plaintiff, on behalf of himself and the Nationwide Class, or in the alternative, the Minnesota Subclass)

220. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

221. This count is brought on behalf of the Minnesota Subclass.

222. Defendant is a "Patient Information Service" as defined by Minn. Stat. § 144.291(Sub-2)(h), a "Provider" as defined by Minn. Stat. § 144.291(Sub-2)(i), and/or a "Related Health Care Entity" as defined by Minn. Stat. § 144.291(Sub-2)(k).

223. Plaintiff and Class members are "Patients" as defined by Minn. Stat. § 144.291(Sub-2)(g).

224. The Plaintiff's and Class members' Personal and Medical Information that was the subject of the Data Breach included "Health Records" as defined by Minn. Stat. § 144.291(Sub-2)(c).

225. The Plaintiff's and Class members' Personal and Medical Information that was the subject of the Data Breach included "Identifying Information" as defined by Minn. Stat. § 144.291(Sub-2)(d).

226. The Plaintiff's and Class members' Personal and Medical Information that was the subject of the Data Breach included information in an "Individually Identifiable Form" as defined by Minn. Stat. § 144.291(Sub-2)(e).

227. In violation of the Minnesota Health Records Act, Defendant failed to protect and allowed the disclosure of the Health Records of Plaintiff and Class members without first obtaining consent or authorization.

228. In violation of the Minnesota Health Records Act, Defendant negligently or intentionally released Health Records of Plaintiff and Class members.

229. As a direct and proximate result of Defendant's violation of Minn. Stat. §144.291 *et seq*., Plaintiff and Class members now face an increased risk of future harm.

230. As a direct and proximate result of Defendant's violation of Minn. Stat. §144.291 *et seq*., Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all Class members, respectfully requests that the Court enter judgment in his favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel under Federal Rule of Civil Procedure 23;

B. Awarding Plaintiff and Class members appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and Class members equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and Class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and Class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and Class members such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: July 25, 2024

Respectfully submitted,

By: /s/E. Michelle Drake

E. Michelle Drake, Bar No. 0387366
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
T. 612.594.5999
F. 612.584.4470
emdrake@bm.net

Steven A. Schwartz*

steveschwartz@chimicles.com
Beena M. McDonald*
bmm@chimicles.com
Alex M. Kashurba*
amk@chimicles.com
Marissa N. Pembroke*
mnp@chimicles.com
CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500

**pro hac vice* to be submitted

Counsel for Plaintiff and the Proposed Class